

07-19-04

10/788, 417

KUMAGAI et al.

March 1, 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

McDermott Will & Emery LLP

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 0 月 1 0 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 3 5 1 5 0 9
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 3 5 1 5 0 9]

出 願 人 株式会社日立製作所
Applicant(s):

BEST AVAILABLE COPY

CERTIFIED COPY OF
PRIORITY DOCUMENT

2 0 0 4 年 3 月 1 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫

出証番号 出証特 2 0 0 4 - 3 0 1 4 9 5 8

【書類名】 特許願
【整理番号】 K03010131A
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/00
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 熊谷 洋子
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 藤城 孝宏
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 鍛 忠司
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 羽根 慎吾
【発明者】
 【住所又は居所】 東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所公共シ
 ステム事業部内
 【氏名】 下之蘭 仁
【特許出願人】
 【識別番号】 000005108
 【氏名又は名称】 株式会社 日立製作所
【代理人】
 【識別番号】 100075096
 【弁理士】
 【氏名又は名称】 作田 康夫
【手数料の表示】
 【予納台帳番号】 013088
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

証明書の有効性確認局装置において、依頼に応じて行う、公開鍵証明書の有効性確認方法であって、

予め、パスの検索と、検索したパスの検証と、を行うステップと、

前記検索と検証の結果を、予め定めた基準に基づき、前記パスを分類して、データベースに登録する、パス登録ステップと、

端末装置から公開鍵証明書の有効性確認依頼を受け取り、予め登録されたパスを用いて検証する、有効性確認ステップと、を有する。

【請求項 2】

請求項 1 記載の公開鍵証明書の有効性確認方法であって、

前記有効性確認ステップにおいて、当該有効性確認依頼に対応する有効なパスが登録されていない場合、新たにパス検索、および検証をすることにより、前記公開鍵証明書の有効性確認を行う。

【請求項 3】

請求項 1 記載の公開鍵証明書の有効性確認方法であって、

前記パス登録ステップにおいて、前記予め定めた基準とは、検証結果に応じて、有効なパスか、有効でないパスかであり、

前記有効性確認ステップにおいて、当該有効性確認依頼に対応するパスが、有効なパス、または有効でないパスとして、前記データベースに登録されている場合は、前記登録結果に従って、前記依頼された公開鍵証明書の有効性確認を行う。

【請求項 4】

請求項 3 記載の公開鍵証明書の有効性確認方法であって、

前記有効性確認ステップにおいて、当該有効性確認依頼に対応するパスが、有効なパスとして登録されている場合でも、当該公開鍵証明書または当該パスに含まれる公開鍵証明書に、制限事項が記述されている場合は、前記有効性確認依頼に応じてパス検証を行い、当該公開鍵証明書および当該パスが前記制限事項を満たしているかどうかを調べるステップと、

制限事項を満たしていれば、有効なパスと判断するステップと、を有する。

【請求項 5】

請求項 3 記載の公開鍵証明書の有効性確認方法であって、

前記有効性確認ステップにおいて、当該有効性確認依頼に対応するパスが、有効なパスとして登録されている場合でも、当該有効性確認依頼または当該公開鍵証明書または当該パスに含まれる公開鍵証明書に、ポリシーが記載されている場合は、前記有効性確認依頼に応じてパス検証を行い、当該公開鍵証明書および当該パスが、電子手続きのポリシーを満たしているかどうかを調べるステップと、

前記ポリシーを満たしている場合に、有効なパスと判断するステップと、を有する。

【請求項 6】

請求項 3 記載の、公開鍵証明書の有効性確認方法であって、

前記パス登録ステップは、トラストアンカー認証局から、エンドエンティティ証明書を発行する認証局までのパスを検索するステップと、

当該エンドエンティティ証明書を発行する認証局が発行する、エンドエンティティ証明書に関する失効リストを取得、検証するステップと、

当該失効リストの検証結果とともに、失効リストに登録するステップと、を有する。

【請求項 7】

請求項 6 記載の公開鍵証明書の有効性確認方法であって、

前記有効性確認ステップにおいて、当該有効性確認依頼に対応するパスが、前記データベースに有効なパスとして登録されている場合、前記失効リストの検証を行わずに、当該公開鍵証明書が失効していないことを確認する。

【書類名】明細書

【発明の名称】公開鍵証明書検証の高速化方法、および装置

【技術分野】

【0001】

本発明は、公開鍵基盤（Public Key Infrastructure：以下PKIという）において、ある端末が受け取った電子手続に対する署名を検証するための公開鍵証明書に関して、その有効性を確認するのに好適な技術に関する。

【背景技術】

【0002】

民間系、公共系の様々な組織、団体において、従来、書面で行ってきた様々な手続を電子化すべく、PKIの導入、整備が進んでいる。

【0003】

図12は、PKIにおいて、認証局（Certificate Authority：以下CAという）が複数ある場合における各CAの関係の例を示している。

【0004】

図示するように、公開鍵証明書の発行とその管理を行う各CAは、ルートCA1を頂点とするツリー構造を持つグループを形成している。このグループはセキュリティドメインと呼ばれており、1つのポリシー管理機関の基で運用されるPKIの単位である。ルートCA1は、自身より1つ下流側に位置する各CA2₁～CA2_nに対して公開鍵証明書を発行する。また、CA2₁～CA2_n各々は、自身より1つ下位に位置する各CA3₁～CA3_{n₁}に対して公開鍵証明書を発行する。このように、ツリー上、1つ上位に位置するCAが自身より1つ下位側に位置するCAに対して公開鍵証明書を発行する。そして、ツリー上、最下位に位置するCA（以下、エンドエンティティ証明書発行CAと呼ぶ）CA s₁～CA s_{n_m}は、電子手続を行うユーザ（以下、End Entity：EEと呼ぶ）EE₁～EE_xに対して公開鍵証明書を発行する。

【0005】

EE₁～EE_x 各々の装置が電子文書の署名を生成する際に使用する秘密鍵（署名鍵）の正当性は、自身を収容する端末収容認証局CA s₁～CA s_{n_m}が発行した公開鍵証明書によって証明され、端末収容認証局CA s₁～CA s_{n_m} 各々の装置が発行する公開鍵証明書の署名を生成する際に使用する秘密鍵の正当性は、自身を収容する認証局CA（s-1）₁～CA（s-1）_{n（m-1）}が発行した公開鍵証明書によって証明される。したがって、EE₁～EE_x 各々の装置が署名を生成する際に使用する秘密鍵は、最終的に、ルート認証局CA1が発行する公開鍵証明書によって証明される。このEE₁～EE_xの装置が署名を生成する際に使用する鍵の正当性を最終的に証明する認証局、云いかえれば、EE₁～EE_xが信頼する、ツリー上、最上位のCAをトラストアンカーCAと呼ぶ。

【0006】

さて、図12において、EE₁装置は、EE_x装置に送信すべき電子文書に対して、EE₁が保持する自身の秘密鍵で署名を行う。そして、署名した電子文書に、CA s₁が発行した前記秘密鍵と対のEE₁の公開鍵証明書を添付して、EE_x装置に送信する。

【0007】

EE_x装置は、EE₁装置から受け取った電子文書の署名を、当該電子文書に添付されたEE₁の公開鍵証明書を用いて検証することができる。しかし、EE₁の公開鍵証明書はEE_xの証明書発行CA s_{n_m}が発行したものではないので、EE_xは、自身のトラストアンカーCAであるルートCA1によって当該公開鍵証明書の有効性が証明されるものであることを確認しなければ、当該公開鍵証明書を信頼することはできない。この公開鍵証明書の有効性確認処理は、以下の手順によって行われる。

(1) トラストアンカーCAから公開鍵証明書の発行元CAまでのパスの検索

トラストアンカーCA（ここでは、ルートCA1）を起点CAとし、起点CAが発行した公開鍵証明書の発行先を調べ、当該発行先にCAが含まれる場合は当該CAが発行した

公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先に、E E 証明書発行 C A（ここでは、E E₁ の公開鍵証明書を発行する C A s₁）が含まれるまで続け、トラストアンカー C A から E E 証明書発行 C A までのパスを検索する。

（2）検索したパスの検証

上記（1）により検索したパス上の各 C A から、パス上において当該 C A の 1 つ下位側の C A に対して発行した公開鍵証明書を入手する。そして、有効性確認対象の公開鍵証明書（ここでは、E E 証明書発行 C A s₁ が E E₁ に対して発行した公開鍵証明書）の署名を、当該公開鍵証明書を発行した C A（ここでは、E E 証明書発行 C A s₁）より 1 つ上位の C A が発行した公開鍵証明書で検証し、検証できた場合は、当該 1 つ上位の C A が発行した公開鍵証明書の署名をさらに 1 つ上位の C A が発行した公開鍵証明書で検証する処理を、当該 1 つ上位の C A がトラストアンカー C A となるまで続ける。そして、このような公開鍵証明書の署名検証がトラストアンカーまでできた場合に、有効性確認対象の公開鍵証明書の有効性が確認されたものとする。

【0008】

E E_x 装置は、E E₁ 装置より受け取った電子文書の署名を当該電子文書に添付された E E₁ の公開鍵証明書をを用いて検証すると共に、上記の（1）、（2）に示す手順に従い当該電子文書の署名検証に用いた E E₁ の公開鍵証明書の有効性を確認することにより、当該電子文書の正当性を確認することができる。

【0009】

なお、以上では、公開鍵証明書の有効性確認処理を E E 装置で行うことを前提としている。しかし、公開鍵証明書の有効性確認処理は負荷が重く、これを E E で行うためには、当該 E E 装置に高い処理能力が要求される。そこで、ネットワークを介して E E 装置に接続された証明書の有効性確認局（以下、Validation Authority: V A という）を設け、当該 V A 装置に、当該 E E の代わりに公開鍵証明書の有効性確認を行わせることが、インターネットに関するさまざまな技術の標準化を定める団体である I E T F（Internet Research Task Force）により提案されている。V A 装置において、公開鍵証明書の有効性確認を行う場合、まず E E 装置は公開鍵証明書の有効性確認依頼を、V A 装置に送付する。次に、V A 装置において、上記（1）、（2）の処理を行い、最後に、その結果を E E 装置に送付する。

【0010】

このとき、E E 装置が公開鍵証明書の有効性確認を依頼してから、その結果が分かるまでにかかる時間を短くするための方法として、次のようなものがある。

【0011】

V A 装置において、予め定期的にパスを検索し、パスデータベースに登録しておく。そして、ある E E 装置から公開鍵証明書の有効性確認の依頼があった場合に、V A 装置のパスデータベースに、対応するパスを検索し、検索したパスの検証を行うことにより、前記公開鍵証明書の有効性を確認する（例えば特許文献 1 を参照）。

【0012】

また、もう 1 つの方法では、V A 装置において、予め定期的に全てのパスを検索し、検索したパスの検証を行う。検証が成功したパス（有効なパス）についてのみ、パスデータベースに登録しておく。そして、ある E E 装置から公開鍵証明書の有効性確認の依頼があった場合に、V A 装置のパスデータベースに、対応するパスが登録されているか否かを調べることで、前記公開鍵証明書の有効性を確認する（例えば特許文献 2 を参照）。

【0013】

【特許文献 1】 米国特許第 6 1 3 4 5 5 0 号明細書

【0014】

【特許文献 2】 米国特許出願公開第 2 0 0 2 / 0 4 6 3 4 0 号明細書

【発明の開示】

【発明が解決しようとする課題】

【0015】

上記特許文献2に記載されていた方法では、E E装置から受け取った公開鍵証明書の有効性確認依頼に対応するパスが、パスデータベースに登録されていない場合は、有効性確認対象証明書が有効でないものと判断していた。しかし、この方法に従うと、パス検索時に存在しなかったパスが、E E装置からの公開鍵証明書の有効性確認依頼を受け取った時に、新たに存在する場合には、有効な公開鍵証明書を有効でないと判断してしまうことがある。上記特許文献2には、このような場合の処理については記述されていなかった。

【0016】

また、上記特許文献1にも、E E装置から受け取った公開鍵証明書の有効性確認依頼に対応するパスが、パスデータベースに登録されていない場合の処理については記述されていなかった。

【0017】

このような、V Aで受け付けた有効性確認依頼に対応するパスがパスデータベースに登録されていない場合に、新たにパス検索、検証を行うことで適切な結果を応答することができる。しかし、この場合の有効性確認処理時間が長くなってしまいう課題がある。

【0018】

現在、民間系、公共系のさまざまな組織、団体において、P K Iの導入、整備が進んでおり、その結果、多数のセキュリティドメインが並列し、複雑なP K I構成となることが予想される。さらに、P K Iを利用したアプリケーションが普及すると、たくさんの有効性確認依頼がなされると予想される。このような場合、E Eが公開鍵証明書の有効性確認を依頼してから、その結果が分かるまでにかかる時間が長くなり、サービスの低下を招いてしまう。

【課題を解決するための手段】

【0019】

本発明は、パス検索時に存在しなかったパスが、パス検索時より後に形成された場合でも適切な結果を応答する技術、および／または、E Eが公開鍵証明書の有効性確認を依頼してからその結果が分かるまでにかかる時間をさらに短くする技術を提供する。

【0020】

具体的には、本発明では、ネットワークを介して、複数の端末装置（E E装置）やC A装置に接続されたV A装置は、あるE E装置からの依頼に応じて、公開鍵証明書の有効性を確認するために以下の処理を行う。

【0021】

公開鍵証明書を発行することにより関係付けられた全てのC Aに関して、存在するパスを全て検索し、前記パス検索により検出されたパスについて検証を行う。また、検出したパスの端点に位置するE E証明書発行C Aが発行する、E E証明書に関する失効リスト（Certificate Revocation List, 以下C R Lという）を取得する。取得したC R Lについて、当該C R Lが有効期間内であることを確認するとともに、当該C R Lの発行C Aの公開鍵証明書により、当該C R Lの署名検証を行う。そして、検証できたパスと、検証できなかったパスを、分類して、パスデータベースに登録する。このパスデータベース作成処理は、E Eからの公開鍵証明書の有効性確認依頼とは独立して、所定の規則に従って、繰り返し、例えば定期的に行う。

【0022】

そして、あるE Eから、公開鍵証明書の有効性確認依頼があった場合に、それに対応するパスが、パスデータベースに登録されているか否かを調べ、検証できたパスとしてデータベースに登録されている場合は、データベースに登録されたC R Lを用いて、当該公開鍵証明書が失効しているか否かを確認することにより、当該公開鍵証明書の有効性を確認する。

【0023】

一方、当該公開鍵証明書に対応するパスが、検証できなかったパスとしてパスデータベースに登録されている場合は、当該登録されている有効でないパス以外に、有効なパスが存在するかどうかを調べ、存在しない場合には、当該公開鍵証明書は検証できなかったも

のとする。新たなパスやCRLを検出した場合には、当該パスや当該CRLを用いて当該公開鍵証明書の有効性を確認し、当該検証結果をもとに、パスデータベースに追加登録を行う。

【0024】

また、有効性確認依頼があった公開鍵証明書に対応するパスやCRLが、パスデータベースに登録されていない場合は、新たにパスやCRLの検索、検証処理を行うことにより、上記公開鍵証明書の有効性を確認する。このとき、新たなパスやCRLを検出した場合には、当該パスや当該CRLの検証結果をもとに、パスデータベースに追加登録を行う。

【0025】

本発明によれば、あるEEから公開鍵証明書の有効性確認依頼を受けた場合に、パス検索時より後に新たなパスが形成された場合でも、適切な結果を応答することができる。かつ、有効性確認依頼に対応するパスが、検証できたパスとして登録されている場合には、上記の(1)、(2)に示した、当該EEのトラストアンカーCAから当該公開鍵証明書のEE証明書発行CAまでのパスの検索、検出したパスの検証、および、当該公開鍵証明書に対応するCRLの署名検証を行う必要がない。また、有効性確認依頼に対応するパスが、検証できなかったパスとして登録されている場合には、パス検索、検証を、少ない処理で行うことができる。したがって、あるEEが、公開鍵証明書の有効性確認を依頼してから、当該有効性が確認されるまでにかかる時間を短縮できる。

【発明の効果】

【0026】

本発明によれば、パス検索時より後に新たなパスが形成された場合でも、適切な結果を応答することができ、および／または、EEが公開鍵証明書の有効性確認を依頼してからその結果が分かるまでにかかる時間を短縮することができる。

【発明を実施するための最良の形態】

【0027】

図1は、本発明の一実施形態が適用されたPKIシステムの概略構成を示す図である。

【0028】

本実施例のPKIシステムは、電子的に手続を行う複数のEE₁装置(11)～EE_N装置(11)(EE装置(11)と総称する)と、公開鍵証明書発行業務を行うCA₁装置(13)～CA_M装置(13)と、公開鍵証明書の有効性確認局VA(14)と、それぞれを接続するインターネット等のネットワーク(以下、NETという)16からなる。

【0029】

図2は、図1に示すPKIシステムでの各CAの関係の一例を示す図である。

【0030】

図示するように、本実施形態のPKIシステムでは、民間系、政府系といった複数のセキュリティドメインSD(SD1～SD2)が並存していることを前提としている。また、各セキュリティドメインSDのルートCA(図2ではCA₁₁、CA₂₁、)は、例えば、ブリッジ認証局CAbridgeに対して公開鍵証明書を発行すると共に、CAbridgeから公開鍵証明書を発行してもらうことにより、CAbridgeとの間で相互認証を行っているものとする。このようにすることで、あるセキュリティドメインSDに属するCAと他のセキュリティドメインSDに属するCAとの間に、一方のCAが発行した公開鍵証明書の有効性を、他方のCAにて確認できるようにするためのパスが形成される。

【0031】

次に、図1のPKIシステムを構成する各装置について説明する。

【0032】

まず、図3を用いて、EE装置(11)を説明する。

【0033】

EE装置(11)は、処理部30aと記憶部30bと、NET16を介して他装置と通信を行うための通信部30cと、ユーザ(EE)が作成した電子文書や他のEEから受け

取った電子文書の入出力やユーザからの指示の受付を行う入出力部 3 0 d と、を有する。

【0 0 3 4】

処理部 3 0 a は、電子文書に対する署名を生成する署名生成部 3 1 と、署名の検証を行う署名検証部 3 2 と、E E 装置の各部を統括的に制御する制御部 3 3 と、を有する。

【0 0 3 5】

記憶部 3 0 b は、利用者が作成した電子文書を保持する電子文書保持部 3 4 と、秘密鍵（署名鍵）と、これと対になる公開鍵の公開鍵証明書と、当該 E E 装置を運用する E E が信頼する C A の自己署名証明書を保持する鍵保持部 3 5 と、他の E E から受け取った署名付きの電子文書と公開鍵証明書を保持する検証対象保持部 3 6 と、を有する。

【0 0 3 6】

このような構成において、制御部 3 3 は、入出力部 3 0 d を介してユーザから、電子文書保持部 3 4 に保持してある電子文書を他の E E に送信すべき旨の指示を受け付けると、当該電子文書を電子文書保持部 3 4 から読み出し、これを署名生成部 3 1 に渡す。署名生成部 3 1 は、鍵保持部 3 5 に保持されている秘密鍵を用いて渡された当該電子文書に対する署名を生成する。

【0 0 3 7】

制御部 3 3 は、電子文書保持部 3 4 から読み出した電子文書に署名生成部 3 1 で生成された署名を付して、署名付き電子文書を作成し、作成した署名付き電子文書と鍵保持部 3 5 に保持されている公開鍵証明書とを、通信部 3 0 c を介して、ユーザから指示された送信先の E E 装置へ送信する。制御部 3 3 は、通信部 3 0 c を介して、他の E E 装置から署名付き電子文書と公開鍵証明書を受け取ると、これらに関連づけて検証対象保持部 3 6 に保持させると共に、これらの検証要求を署名検証部 3 2 に通知する。

【0 0 3 8】

これを受けて、署名検証部 3 2 は、検証対象保持部 3 6 に保持されている署名付き電子文書の署名を、対応する公開鍵証明書を用いて検証する。署名検証部 3 2 は、V A 装置（1 4）に、上記の署名検証に用いた公開鍵証明書の有効性の確認依頼を送信する。この際、必要に応じて、前記署名付き電子文書により行おうとしている電子手続に関するポリシー（例えば、取引額等の信頼度）の検証依頼を、前記確認依頼に含める。そして、V A 装置（1 4）において、上記ポリシーの検証も含めた当該公開鍵証明書の有効性が確認された場合にのみ、署名付き電子文書を正当なものとして扱い、必要に応じて入出力部 3 0 d から出力する。

【0 0 3 9】

次に、図 4 を用いて C A 装置（1 3）を説明する。

【0 0 4 0】

C A 装置（1 3）は、処理部 4 0 a と、記憶部 4 0 b と、N E T 1 6 を介して他装置と通信を行うための通信部 4 0 c と、公開鍵証明書等の入出力や当該装置の操作者からの指示の受付や処理結果の出力を行う入出力部 3 0 d と、を有する。

【0 0 4 1】

処理部 4 0 a は、公開鍵証明書を発行する発行部 4 1 と、発行部 4 1 が発行した公開鍵証明書の管理を行う管理部 4 2 と、C A 装置の各部を統括的に制御する制御部 4 3 と、を有する。

【0 0 4 2】

記憶部 4 0 b は、発行部 4 1 が発行した公開鍵証明書を保持する公開鍵証明書データベース 4 4 と、公開鍵証明書データベース 4 4 に保持されている各公開鍵証明書の発行先が記述されていた発行先管理リストを保持する発行先管理リスト保持部 4 5 と、失効証明書リスト保持部 4 6 と、を有する。

【0 0 4 3】

このような構成において、制御部 4 3 は、入出力部 4 0 d あるいは通信部 4 0 c を介して公開鍵証明書の発行依頼を受け付けると、その旨を発行部 4 1 に伝える。これを受けて、発行部 4 1 は、これに対する公開鍵証明書を作成する。この際、C A の秘密鍵で公開鍵

証明書に署名をする。また、必要に応じて、公開鍵証明書中に、当該公開鍵証明書の有効期限や、信頼しない他の認証局の名称 (Name Constraints) や、当該公開鍵証明書の有効性確認のために許容される最大パス長 (パス上の許容最大認証局数) や、電子手続の取引額等を表したポリシーを記述する。そして、作成した公開鍵証明書を入力部 40d あるいは通信部 40c を介して、郵送あるいは通信により、発行依頼元に渡す。また、この公開鍵証明書を公開鍵証明書データベース 44 に登録すると共に、その発行先 (つまり発行依頼元) の情報を、発行先管理リスト保持部 45 に保持されている発行先管理リストに記述する。

【0044】

制御部 43 は、入出力部 40d あるいは通信部 40c を介して、公開鍵証明書の失効依頼を受け付けると、その旨を管理部 42 に伝える。これを受けて、管理部 42 は、失効対象の公開鍵証明書を公開鍵証明書データベース 43 から削除すると共に、当該公開鍵証明書の発行先の情報を、発行先管理リスト保持部 44 に保持されている発行先管理リストから削除する。そして、管理部 42 は、失効依頼により公開鍵証明書データベース 43 から削除した公開鍵証明書に関する情報が記述された失効証明書リストを、定期的に作成し、これを失効証明書リスト保持部 45 に保持させる。なお、管理部 42 は、作成した失効証明書リストに、次の失効証明書リストの作成予定日時を記述するものとする。

【0045】

また、制御部 43 は、通信部 40c を介して、他装置より公開鍵証明書の失効情報の問い合わせを受け取ると、失効証明書リスト保持部 45 に保持されている失効証明書リストを検索して、問い合わせのあった公開鍵証明書が失効しているか否かを調べる。そして、その結果を、通信部 40c を介して、問い合わせをした他装置に応答することもできる。(このような問い合わせと応答に用いる通信プロトコルとして、OSCP (Online Certification status protocol) がある)。

【0046】

管理部 42 は、公開鍵証明書データベース 44 に格納されている各公開鍵証明書の有効期限を調査し、有効期限を過ぎている公開鍵証明書の発行先の情報を、発行管理リスト保持部 45 に保持されている発行先管理リストから削除する処理も行う。

【0047】

次に、図 5 を用いて、VA 装置 (14) を説明する。

【0048】

図示するように、VA 装置 (14) は、処理部 50a と、記憶部 50b と、ネットワーク NET 16 を介して他装置と通信を行うための通信部 50c と、公開鍵証明書等の入出力やユーザよりの指示の受け付けを行う入出力部 50d と、を有する。

【0049】

処理部 50a は、パス検索部 51 と、パス検証部 52 と、有効期限/失効状態調査部 53 と、有効性確認部 54 と、VA 装置の各部を統括的に制御する制御部 55 と、を有する。また、記憶部 50b は、パスデータベース 56 と、失効証明書リスト作成予定日時データベース 57 とを有する。このうちパスデータベース 56 は、有効なパスデータベース 56A と、有効でないパスデータベース 56B と、を有する。

【0050】

パス検索部 51 は、例えば定期的に、任意の CA をトラストアンカー CA として、当該トラストアンカー CA から、EE 証明書を発行する全ての EE 証明書発行 CA までのパスを検索する。また、検出したパスの EE 証明書発行 CA が発行する、EE 証明書に関する失効証明書リスト (CRL) を取得する。トラストアンカー CA は、全ての CA、または設定を設けることにより一部の CA として、検索を行うことができる。

【0051】

パス検証部 52 は、パス検索部 51 でパスの検索が行われる毎に、当該パス検索部 51 で検出されたパスの検証を行う。また、パス検索部 51 において当該パスに対応する CRL を取得できた場合には、当該 CRL の検証を行う。そして、当該パスの両端に位置する

こととなる、トラストアンカーCAの名称と、EE証明書発行CAの名称とのペアに対応付けて、当該パスを構成する各CA名と、各証明書と、EE証明書に関するCRLとを、当該検証結果に応じて、有効なパスデータベース56A、または有効でないデータベース56Bに登録する。

【0052】

有効期限/失効状態調査部53は、有効なパスデータベース56Aに登録されているパス各々について、当該パスを構成する各公開鍵証明書の有効期限や失効の有無を調査する。そして、その結果に応じてパスデータベース56を更新する。また、有効期限/失効状態調査部53は、各CAの失効証明書リスト保持部46から入手した失効証明書リストに記述されている次の失効証明書リスト作成予定日時を当該CAに対応付けて、失効証明書リスト作成予定日時データベース57に登録する。

【0053】

有効性確認部54は、EE装置からの依頼に従い、トラストアンカーCAを信頼の起点として、公開鍵証明書の有効性の確認を行う。

【0054】

なお、図3～図5に示すEE装置(11)、CA装置(13)とVA装置(14)の各々は、例えば、図6に示すような、CPU61と、メモリ62と、ハードディスク等の外部記憶装置63と、CD-ROM等の可搬性を有する記憶媒体69から情報を読み取る読み取り装置64と、NET16を介して他装置と通信を行うための通信装置65と、キーボードやマウス等の入力装置66と、モニタやプリンタ等の出力装置67と、これらの各装置間のデータ送受を行うインタフェース68とを備えた、一般的な電子計算機上に構築できる。

【0055】

そして、CPU61が外部記憶装置63からメモリ62上にロードされた所定のプログラムを実行することにより、上述の各処理部を実現できる。すなわち、通信部30c、40c、50cは、CPU61が通信装置66を利用することにより、入出力部30d、40d、50dは、CPU61が入力装置66や出力装置67や読み取り装置64を利用することにより、そして、記憶部30b、40b、50bは、CPU61がメモリ62や外部記憶装置63を利用することにより実現される。また、処理部30a、40a、50aは、CPU61のプロセスとして実現される。

【0056】

上記所定のプログラムは、予め外部記憶装置63に格納されていても良いし、上記電子計算機が利用可能な記憶媒体69に格納されており、読み取り装置64を介して、必要に応じて読み出され、あるいは、上記電子計算機が利用可能な通信媒体であるネットワークまたはネットワーク上を伝搬する搬送波を利用する通信装置66と接続された他の装置から、必要に応じてダウンロードされて、外部記憶装置63に導入されるものであってもよい。

【0057】

次に、上記構成のVA装置(14)の動作を説明する。

【0058】

本実施形態のVA装置(14)の動作は、パスの検索、検証および管理動作と、公開鍵証明書の有効性の確認動作とに分かれる。

【0059】

図7～図8のフロー図を用いて、VA装置(14)で行われるパスの検索、検証および管理動作を説明する。

【0060】

制御部55は、VAの運営者によって定められた所定時間(例えば1日)を経過すると(ステップS1001)、パスデータベース56の登録内容を一旦クリアし(ステップS1002)、パス検索部51にパス検索を依頼する。これを受けて、パス検索部51は、任意のCAをトラストアンカーCAとしたときの、EE証明書発行CAまでのパスを検索

する（ステップS1003）。

【0061】

具体的には、パス検索部51は、トラストアンカーCAにアクセスし、トラストアンカーCAが発行し、発行先管理リスト保持部45に保持されている、公開鍵証明書の発行先の情報を入手する。そして、入手した各発行先がCAの場合は、各発行先にアクセスして、発行先管理リスト保持部45に保持されている、各CAが発行した公開鍵証明書の発行先をさらに調べる。この処理を、公開鍵証明書の発行先がEEとなるまで続けることにより、トラストアンカーCAからEE証明書発行CAまでのパスを検索する。ここで、パスのループにより上記の処理が無限に繰り返されるのを防止するため、あるCAから入手した発行先に、それまでに形成された部分パスに存在するCAが含まれる場合は、当該CAを発行先とした上記の処理を行わないものとする。また、パスの端点に位置するEEへ証明書を発行したCAが発行するCRLを取得する。

【0062】

ステップS1003でのパス検索処理を、各CAが図2に示す関係にある場合を例に取り、より具体的に説明する。

【0063】

まず、パス検索部51は、トラストアンカーCAをCAbridgeとしてパス検索を行う。パス検索部51は、CAbridgeにアクセスし、発行先管理リスト保持部45に保持されている、CAbridgeが発行した公開鍵証明書の発行先の情報として、CA₁₁、CA₂₁の情報を入手する。

【0064】

次に、パス検索部51は、CAbridgeから入手した発行先（CA₁₁、CA₂₁）のうちのいずれか1つに注目して、以下の処理を実行する。すなわち、注目した発行先がCA（以下、注目CAと呼ぶこととする）であるならば、CAbridge-注目CAという部分パスを設定する。そして、注目CAの発行先管理リスト保持部45にアクセスして、当該注目CAが発行した公開鍵証明書の発行先の情報をさらに入手する。ここでは、注目した発行先がCA₁₁であるとして、CAbridge-CA₁₁という部分パスを設定し、CA₁₁から、発行先の情報として、CAbridge、CA₁₂、CA₁₃の情報を入手したものとする。

【0065】

次に、パス検索部51は、認証局CA₁₁から入手した発行先（CAbridge、CA₁₂、CA₁₃）に、部分パス上のCA（以下、ループCAと呼ぶこととする）が含まれているか否かを調べる。含まれている場合はその発行先を注目対象から除外する。したがって、ここでは、CAbridgeを注目対象から除外することになる。次に、パス検索部51は、CA₁₁から入手した発行先にEEが含まれるか否かを調べる。あるCAが発行した証明書の発行先にEEが含まれている場合、そのCAはEE証明書発行CAとなる。しかし、CA₁₁から入手した発行先にEEは含まれていないので、CA₁₁はEE証明書発行CAではない。したがって、CAbridge-CA₁₁という部分パスを、EE証明書発行CAまで延長すべく、CA₁₁から入手した、ループCAを除く発行先（CA₁₂、CA₁₃）のうちのいずれか1つに注目する。

【0066】

注目した発行先がCAであるならば、それまでに設定した部分パスにこの注目CAを接続した部分パスを設定する。そして、この注目CAの発行先管理リスト保持部45にアクセスして、当該注目CAが発行した公開鍵証明書の発行先の情報をさらに入手する。ここでは、注目した発行先がCA₁₂であるとして、CAbridge-CA₁₁-CA₁₂というパスを設定し、CA₁₂から、発行先の情報として、EE₁、EE₂を入手したものとする。

【0067】

次に、パス検索部51は、CA₁₂から入手した発行先（EE₁、EE₂）に、ループCAが含まれているか否かを調べる。含まれている場合はその発行先を注目対象から除外

する。ここでは、ループCAは含まれないので、パス検索部51は、次の処理へ移行し、CA₁₂から入手した発行先にEEが含まれるか否かを調べる。ここで、入手した発行先はすべてEEであるので、CA₁₂はEE証明書発行CAである。そこで、このCA₁₂を端点とするパスを、トラストアンカーCA bridgeから、EE証明書発行CA₁₂までのパス(CA bridge-CA₁₁-CA₁₂)として検出する。

【0068】

さらに、パス検索部51は、EE証明書発行CAまでのパスを検出した場合、当該EE証明書発行CA₁₂が発行するCRLを、失効証明書リスト保持部46にアクセスし、取得する。

【0069】

次に、パス検索部51は、検出したパス上の端点に位置するCA₁₂から入手した発行先の情報の中に、未だ注目していない発行先(ループCA以外のCA)があるか否かを調べ、そのような発行先があれば、これを注目CAとして、上記の処理を続ける。一方、そのような発行先がなければ、1つ前に位置するCA₁₁から入手した発行先の情報の中に、未だ注目していない発行先(ループCA以外のCA)があるか否かを調べる。そして、そのような発行先があれば、これを注目CAとして、上記の処理を続ける。ここでは、CA₁₁から入手した発行先の情報のうち、CA₁₃について未だ注目していないので、これを注目CAとして上記の処理を行うことにより、CA bridgeからEE証明書発行CA₁₃までのパス(CA bridge-CA₁₁-CA₁₃)およびCA₁₃が発行するCRLを検出する。

【0070】

このように、パス検索部51は、上記の処理を、検出したパス上に位置する全てのCA各々について、当該CAから入手した発行先の情報の中に、未だ注目していない発行先(ループCA以外のCA)がなくなるまで続けることにより、CA bridgeから各EE証明書発行CAまでのパスを検出する。

【0071】

以上が、任意のCAをトラストアンカーCAとした場合のステップ1003の処理である。

【0072】

後述するように、CA₁₁、CA₂₁各々のCAをトラストアンカーCAとした場合についても、同様にパス検索を行う。

【0073】

制御部55は、パス検索部51によりパスが検出されると(ステップS1004でYes)、パス検証部52にパスの検証を依頼する。これを受けて、パス検証部52は、パス検索部51により検出されたパスの検証を行う(ステップS1005)。

【0074】

具体的には、パス検索部51により検出されたパス各々について、以下の処理を行う。

【0075】

すなわち、まず、パス検証部52は、パス上の各CAの公開鍵証明書データベース44にアクセスし、各CAが当該パス上の1つ次に位置するCA(アクセス先CAがEE証明書発行CAの場合はEE)に対して発行した公開鍵証明書を入手する。

【0076】

次に、パス検証部52は、パスの最後に位置するEE証明書発行CAが発行した公開鍵証明書の署名を、EE証明書発行CAの公開鍵証明書で検証し、検証できた場合は当該EE証明書発行CAの公開鍵証明書の署名をさらに1つ前に位置するCAの公開鍵証明書で検証する。この処理を、当該1つ前に位置する認証局CAがトラストアンカーCAとなるまで続けることにより、当該パスを検証する。さらに、当該EE証明書発行CAが発行するCRLについて、当該EE証明書発行CAの公開鍵証明書で検証する。

【0077】

例えば、図2においてCA bridgeからEE証明書発行CA₁₂までのパス(CA

b r i d g e - C A₁₁ - C A₁₂) および C R L を検証する場合、まず、E E 証明書発行 C A₁₂ の公開鍵証明書の署名を、パス中で C A₁₂ の 1 つ前に位置する C A₁₁ の公開鍵証明書を用いて検証する。そして、検証できた場合は、C A₁₁ の公開鍵証明書の署名を、パス中で C A₁₁ より 1 つ前に位置する C A b r i d g e の公開鍵証明書を用いて検証する。そして、この検証できた場合、さらに、当該 E E 証明書発行 C A₁₂ が発行する C R L について、当該 E E 証明書発行 C A₁₂ の公開鍵証明書で検証する。この、パスおよび C R L の検証できた場合に、C A b r i d g e から E E 証明書発行 C A₁₂ までのパスが仮に検証できたものとする。

【0078】

次に、パス検証部 52 は、パスが仮に検証できたならば、当該パス上の各認証局 C A から入手した公開鍵証明書中に、信頼しない他の認証局の名称 (N a m e C o n s t r a i n s) や当該公開鍵証明書の有効性確認のために許容される最大パス長 (パス上の許容最大認証局数) などの制限の記述があるか否かを調べる。そのような記述がある場合は、当該パスがその制限を満たしているか否かを調べ、満たしている場合にのみ、当該パスが検証できたものとする。

【0079】

さて、制御部 55 は、上記のようにして、パス検索部 51 により検出されたパス各々に対するパス検証部 52 での検証が終了したならば、登録処理を行う。制御部 55 は、パス検証部 52 でパスが検証できた場合 (ステップ S 1006 で Y e s)、当該パスをトラストアンカー C A と、E E 証明書発行 C A と、E E 証明書発行 C A が発行する C R L と、に対応付けて、有効なパスデータベース 56 A に登録し (ステップ S 1007)、ステップ S 1003 へ移行する。また、制御部 55 は、パス検証部 52 でパスが検証できなかった場合 (ステップ S 1006 で N o)、当該パスをトラストアンカー C A と、E E 証明書発行 C A と、E E 証明書発行 C A が発行する C R L と、に対応付けて、有効でないパスデータベース 56 B に登録し (ステップ S 1008)、ステップ 1003 へ移行する。

【0080】

制御部 55 は、ステップ S 1003 ～ステップ S 1008 のステップを、パスが検出されなくなる (ステップ S 1004 で N o) まで繰り返し、パスデータベース 56 を作成する。このとき、全ての C A をトラストアンカーとして、対応する全てのパスを検索する。C A の構成が図 2 の場合は、C A₁₁、C A₂₁、C A b r i d g e の 3 つの C A をトラストアンカーとして、各々に対応する全てのパスを検索する。

【0081】

ステップ S 1003 ～ステップ S 1008 までの処理を行った結果、各 C A が図 2 に示す関係にある場合、パス検索部 51 により検出される、全てのパスは、図 9 に示すとおりとなる。

【0082】

一方、有効期限／失効状態調査部 53 は、有効なパスデータベース 56 A に登録されている公開鍵証明書の中に、有効期限切れの公開鍵証明書があるか否かを調べる (ステップ S 1009)。有効期限切れの公開鍵証明書がある場合は、当該公開鍵証明書の発行元 C A の公開鍵証明書データベース 44 にアクセスして、当該公開鍵証明書の発行先に対して新たに発行された公開鍵証明書を検索する (ステップ S 1010)。

【0083】

そして、そのような公開鍵証明書が前記発行元 C A の公開鍵証明書データベース 44 になれば、前記有効期限切れの公開鍵証明書に対応付けて登録されているパスに関する情報を、有効なパスデータベース 56 A から削除し、有効でないパスデータベース 56 B へ登録する (ステップ S 1011)。一方、そのような公開鍵証明書が前記発行元 C A の公開鍵証明書データベース 44 中にあればこれを入手する。そして、前記有効期限切れの公開鍵証明書に対応付けて、有効なパスデータベース 56 A に登録されているパスの検証を、当該有効期限切れの公開鍵証明書の代わりに新たに入手した公開鍵証明書を用いて、上記のステップ S 1005 と同じ要領で行う (ステップ S 1012)。

【0084】

さて、パスが検証できた場合（ステップS1013でYes）は、当該パスに対応付けられて有効なパスデータベース56Aに登録されている前記有効期限切れの公開鍵証明書を、新たに入手した公開鍵証明書に置き換える（ステップS1014）。一方、パスが検証できなかった場合（ステップS1013でNo）は、前記有効期限切れの公開鍵証明書に対応付けて登録されているパスを、有効なパスデータベース31から削除し、新たに入手した公開鍵証明書に置き換えたパスを、有効でないパスデータベースに置き換える（ステップS1015）。

【0085】

次に、有効期限／失効状態調査部53は、失効証明書リスト作成予定日時データベース57を調べ、既に経過した失効証明書リスト作成予定日時に対応付けられているCAを検索する（ステップS1016）。そのような認証局CAが存在する場合（ステップS1017でYes）は、当該CAの失効証明書リスト保持部46にアクセスして、当該CAが発行した最新の失効証明書リストを入手する（ステップS1018）。そして、失効証明書リスト作成予定日時データベース57にて、当該認証局CAに対応付けて登録されている失効証明書リスト作成予定日時を、入手した最新の失効証明書リストに記述されている失効証明書リスト作成予定日時に更新する（ステップS1019）。

【0086】

それから、有効期限／失効状態調査部53は、入手した最新の失効証明書リストに記述されている公開鍵証明書が、有効なパスデータベース56Aに登録されているか否かを調べ（ステップS1020）、登録されている場合は、当該公開鍵証明書に対応付けられているパスに関する情報を有効なパスデータベース56Aから削除し、有効でないパスデータベース56Bへ登録する（ステップS1021）。

【0087】

次に、公開鍵証明書の有効性の確認動作について説明する。

【0088】

図10～図11は、本実施形態のVA装置（14）で行われる公開鍵証明書の有効性の確認動作を説明するためのフロー図である。

【0089】

制御部55は、通信部50cを介して、EEから、少なくとも当該EEが信頼するトラストアンカーCAの名称を含んだ、他EEの公開鍵証明書の有効性確認依頼を受け取ると（ステップS2001）、その旨を有効性確認部54に通知する。

【0090】

これを受けて、有効性確認部54は、証明書の有効性確認依頼の記述から特定される、トラストアンカーCAと、当該証明書を発行したEE証明書発行CAと、に対応付けられたパスが、有効なパスデータベース56Aに登録されているか否かを調べる（ステップS2002）。

【0091】

その結果、証明書の有効性確認依頼に記述された、トラストアンカーCAと、当該証明書を発行したEE証明書発行CAと、に対応付けられたパスが、有効なパスデータベース56Aに登録されていることが確認できたならば（ステップS2002でYes）、有効性確認部54は、当該パスの端点であるEE証明書発行CAの公開鍵証明書を用いて、EE証明書の署名検証を行う。さらに、有効性確認部54は、当該パスと対応付けられて登録されているCRLを用いて、EE証明書が失効していないかどうかを確認する（ステップS2003）。

【0092】

EE証明書の署名検証が失敗した場合（ステップ2003でNo）、又はEE証明書がCRLに記述され失効されていた場合、有効性確認部54は、EE証明書有効でないものと判断し、その旨を、通信部50cを介して、依頼元のEEに通知する（ステップS2004）。

09)。

【0093】

一方、各証明書には、信頼しない認証局名による制限や、当該公開鍵証明書の有効性確認のために許容される最大パス長（パス上の許容最大認証局数）を記述できる拡張項目がある。ステップ2003で、EE証明書の署名検証および、失効していないかどうかの確認が成功した場合（Yesの場合）、EE証明書および当該パスに含まれる各CAの証明書に、上述の制限が記述されているか否かをさらに調べる（ステップS2004）。

【0094】

そのような制限の記述がない場合、ステップS2006に移行する。

【0095】

そのような制限の記述がある場合は、ステップS2005に移行して、EE証明書がその制限に反していないか否かを調べる。EE証明書が制限事項に反している場合、有効性確認部54は、公開鍵証明書が有効でない旨を、通信部50cを介して、依頼元のEE装置（11）に通知する（ステップS2009）。EE証明書が制限事項に反していない場合は、ステップS2006に移行する。

【0096】

ステップS2006では、有効性確認部54は、EE装置（11）から受け取った確認依頼に、当該EEが行おうとしている電子手続の取引額等を示したポリシーが含まれているか否かを調べる。

【0097】

ポリシーが含まれている場合は、EE証明書および当該パスを構成する各公開鍵証明書中に、前記ポリシーを満たすポリシーの記述があるか否かをさらに調べる（ステップS2007）。

【0098】

EE証明書および当該パスに、前記ポリシーを満たすポリシーの記述がない場合は、EE証明書を、依頼元のEEが行おうとしている電子手続のための公開鍵証明書の有効性確認に利用できないものと判断し、公開鍵証明書が有効でない旨を、通信部50cを介して、依頼元のEE装置（11）に通知する（ステップS2009）。

【0099】

一方、EEから受け取った確認依頼に当該EEが行おうとしている電子手続を示すポリシーが含まれていない場合（ステップS2006でNo）、あるいは、含まれていても、当該パスおよびEE証明書に記述されているポリシーが前記ポリシーを満たす場合（ステップS2007でYes）は、公開鍵証明書は有効であると判断し、公開鍵証明書が有効である旨を、通信部50cを介して、依頼元のEEに通知する（ステップS2008）。

【0100】

また、ステップS2002において、証明書の有効性確認依頼に記述された、トラストアンカーCAと、当該証明書を発行したEE証明書発行CAと、に対応付けられたパスが、有効なパスデータベース56Aに登録されていない場合（ステップS2002でNo）、当該パスが有効でないパスデータベース56Bに登録されているか否かを確認する（ステップS2010）。有効でないデータベース56Bに、当該パスが登録されていない場合（ステップS2010でNo）、図11のステップS2012に移行する。

【0101】

ステップS2012では、パス検索部51が、確認依頼記述されたトラストアンカーCAから、確認対象のEE証明書までのパスを検索する。この検索は、パス検索部51が予め定められた所定の規則に従って行うものとは異なり、臨時に行う。

【0102】

パス検索部51が、トラストアンカーCAから、EE証明書までのパスを検出しなかった場合（ステップS2013でNo）、有効性確認部54は、EE証明書が有効でない旨を、通信部50cを介して、依頼元のEEに通知する（ステップS2019）。一方、パス検索部51が、トラストアンカーCAから、EE証明書までのパスを検出した場合（

ステップS2013でYes)、パス検証部52において、検出したパスを検証する(ステップS2014)。

【0103】

検出したパスが検証できた場合(ステップS2015でYes)、当該パスのトラストアンカーCAから、EE証明書発行CAまでのパスと、EE証明書発行CAが発行するCRLを、有効なパスデータベースへ登録する(ステップS2016)。そして、有効性確認部54は、EE証明書が有効性である旨を、通信部50cを介して、依頼元のEEに通知する(ステップS2017)。

【0104】

一方、ステップ2015において、検出したパスが検証できなかった場合(S2015でNo)、当該パスのトラストアンカーCAから、EE証明書発行CAまでのパスと、EE証明書発行CAが発行するCRLを、有効でないパスデータベースへ登録する(ステップS2018)。そして、ステップS2011へ移行し、これまで検出したパス以外に、パスが存在するかどうか検索を行い、それ以降のステップを同じように実行する。

【0105】

また、図10のステップ2010において、有効でないパスデータベース56Bに、当該パスが登録されていた場合(ステップS2010でYes)、さらに当該登録されていたパス以外に、有効性確認依頼に対応するパスを検出した場合(ステップS2011でYes)、ステップS2014に移行し、当該検出したパスの検証、登録処理を行う(ステップS2014～ステップS2019)。

【0106】

一方、当該登録されていたパス以外に、有効性確認依頼に対応するパスを検出なかった場合(ステップS2011でNo)、有効性確認部54は、公開鍵証明書が有効性でない旨を、通信部50cを介して、依頼元のEEに通知する(ステップS2009)。

【0107】

以上の実施形態では、トラストアンカーCAから各EE証明書発行CAまでのパスの検索および検証を、EEからの公開鍵証明書の有効性確認依頼とは独立した所定の規則に従って、例えば定期的に行う。

【0108】

検索、検証したパスは、有効なパスまたは有効でないパスに分類し、パスデータベースに登録しておく。そして、有効性確認依頼に対応するパスが、有効なパスとして登録されているか、有効でないパスとして登録されているかを調べることにより、当該EE証明書が有効であるか否かを判断する。

【0109】

このとき、当該有効性確認依頼に対するパスが、有効でないパスに登録されている場合は、当該有効でないパス以外に対応するパスがあるかどうかを、検索、検証し、確認を行う。また、当該有効性確認依頼に対するパスが、パスデータベースに登録されていない場合には、パス検索、検証を臨時に行う。したがって、認証局の構成が変化した場合にも、最新のパス情報により検証を行うため、適切な有効性確認結果を応答することができる。また、有効でないパスをキャッシュしておくことにより、公開鍵証明書を受け付けてから、当該有効性を確認するまでにかかる時間を短縮することができる。

【0110】

また、本実施形態では、パスを登録する際に、パスの端点となるEE証明書発行CAが発行するCRLを、当該CRLの検証結果とともに登録しておく。そして、あるEEから公開鍵証明書の有効性確認依頼を受けた場合、当該EE証明書が失効しているかどうかを、当該CRLを用いて確認する。したがって、公開鍵証明書の有効性確認にかかる時間をより短縮することができる。

【0111】

なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【0112】

例えば、上記の実施形態では、VAは、パスをデータベースに登録する際に、有効なパスデータベース56Aと、有効でないパスデータベース56Bの、二つのデータベースに分類して登録している。しかし、一つのデータベースに、当該パスの状態を示すフラグをつけて、有効なパスと、有効でないパスを分類してもよい。

【0113】

また、上記の実施形態では、説明をわかりやすくするため、図2に示すように、EE証明書発行CAはEEに対してのみ公開鍵証明書を発行し、その他のCAはCAに対してのみ公開鍵証明書を発行するものと仮定したが、EEとCAの両方に対して公開鍵証明書を発行するCAを含む場合でも、本発明は適用できる。

【0114】

また、上記の実施形態では、説明を分かりやすくするため、図2に示すように、CAの構成を階層構造と仮定したが、CAの構成がより複雑なメッシュ構造となっている場合でも、本発明は適用できる。

【図面の簡単な説明】

【0115】

【図1】本発明の一実施形態が適用されたPKIシステムの概略構成を示す図である。

【図2】図1に示すPKIシステムでの各CAの関係の一例を示す図である。

【図3】図1に示すEEの概略構成を示す図である。

【図4】図1に示すVAの概略構成を示す図である。

【図5】図1に示すVAの概略構成を示す図である。

【図6】図3～図5に示すEE、CAおよびVAの各々のハードウェア構成例を示す図である。

【図7】図5に示すVAで行われるパスの検索、検証および管理動作を説明するためのフロー図である。

【図8】図5に示すVAで行われるパスの検索、検証および管理動作を説明するためのフロー図である。

【図9】各CAが図2に示す関係にある場合に、VAのパス検索部51で検出される全てのパスを示す図である。

【図10】図5に示すVAで行われる公開鍵証明書の有効性の確認動作を説明するためのフロー図である。

【図11】図5に示すVAで行われる公開鍵証明書の有効性の確認動作を説明するためのフロー図である。

【図12】従来のPKIにおいて、認証局が複数ある場合におけるCAの関係の一例を示す図である。

【符号の説明】

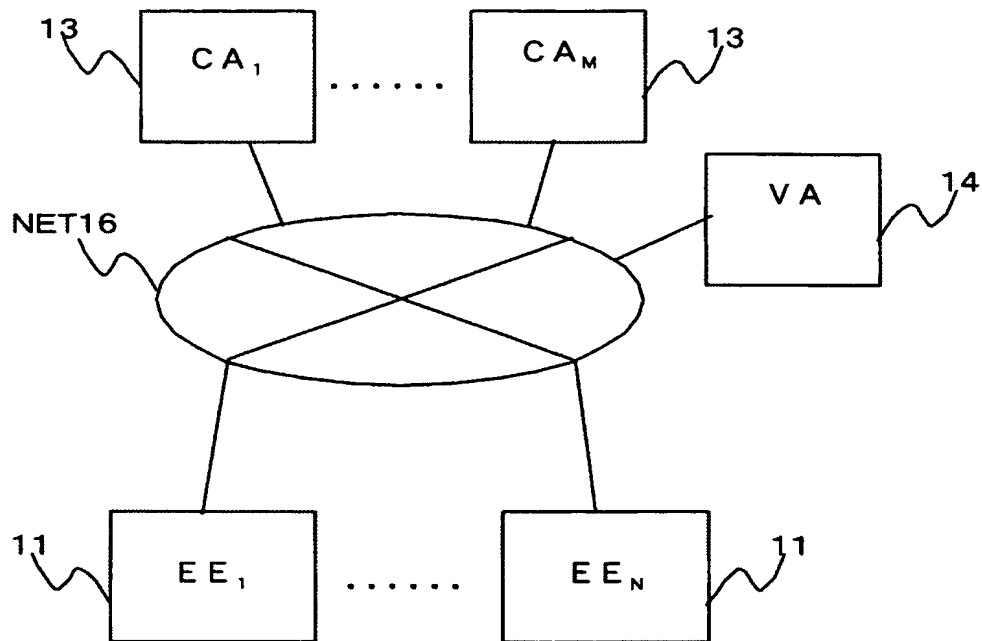
【0116】

CA・・・認証局，VA・・・証明書の有効性確認局，EE・・・エンドエンティティ，SD・・・セキュリティドメイン，11・・・EE₁，12・・・EE_N，13・・・CA₁，14・・・CA_M，15・・・VA，16・・・VA，30a，40a，50a・・・処理部，30b，40b，50b・・・記憶部，30c，40c，50c・・・通信部，30d，40d，50d・・・入出力部，31・・・署名生成部，32・・・署名検証部，33，43，55・・・制御部，34・・・電子文書保持部，35・・・鍵保持部，36・・・検証対象保持部，41・・・発行部，42・・・管理部，44・・・公開鍵証明書データベース，45・・・発行先管理リスト保持部，46・・・失効証明書リスト保持部，51・・・パス検索部，52・・・パス検証部，53・・・有効期限／執行状態調査部，54・・・有効性確認部，56・・・パスデータベース，56A・・・有効なパスデータベース，56B・・・有効でないパスデータベース，57・・・失効証明書リスト作成予定日時データベース，61・・・CPU，62・・・メモリ，63・・・外部記

憶装置、6 4 . . . 読取装置、6 5 . . . 通信装置、6 6 . . . 入力装置、6 7 . . . 出力装置、6 8 . . . インタフェース、6 9 . . . 記憶媒体。

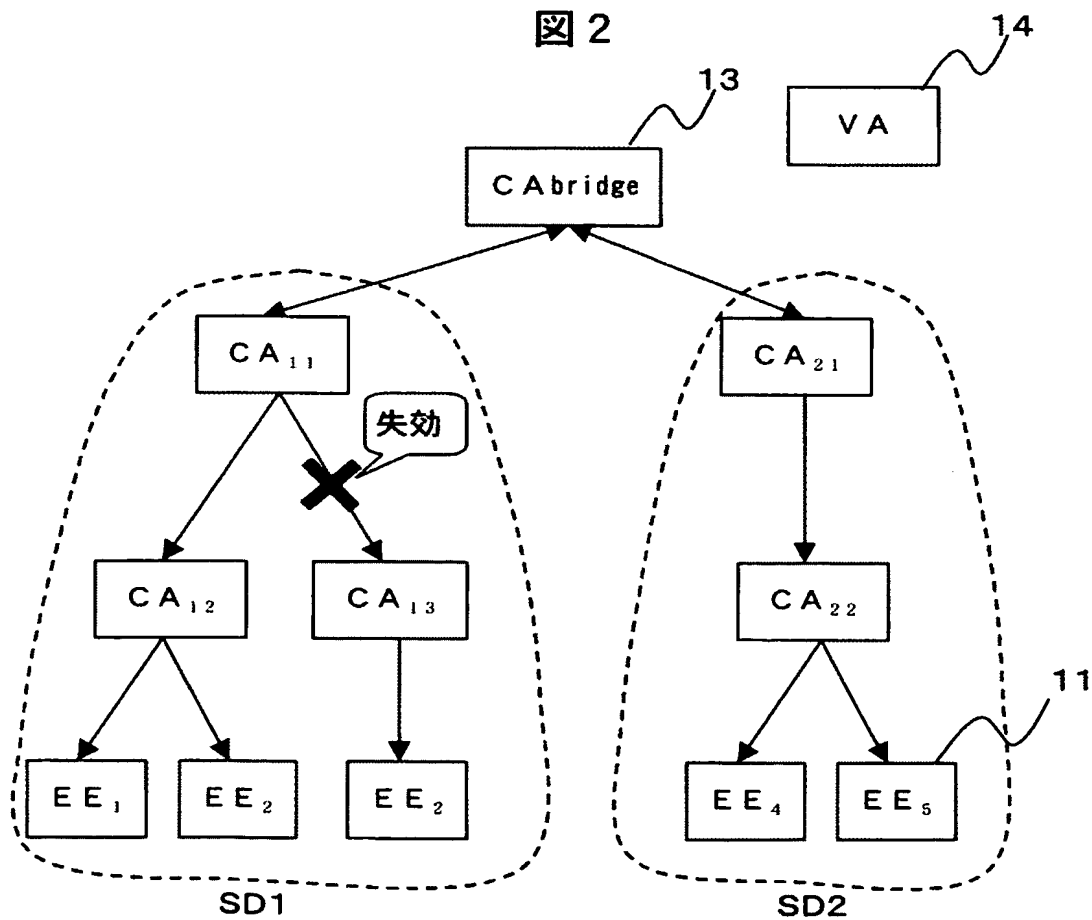
【書類名】 図面
【図 1】

図 1



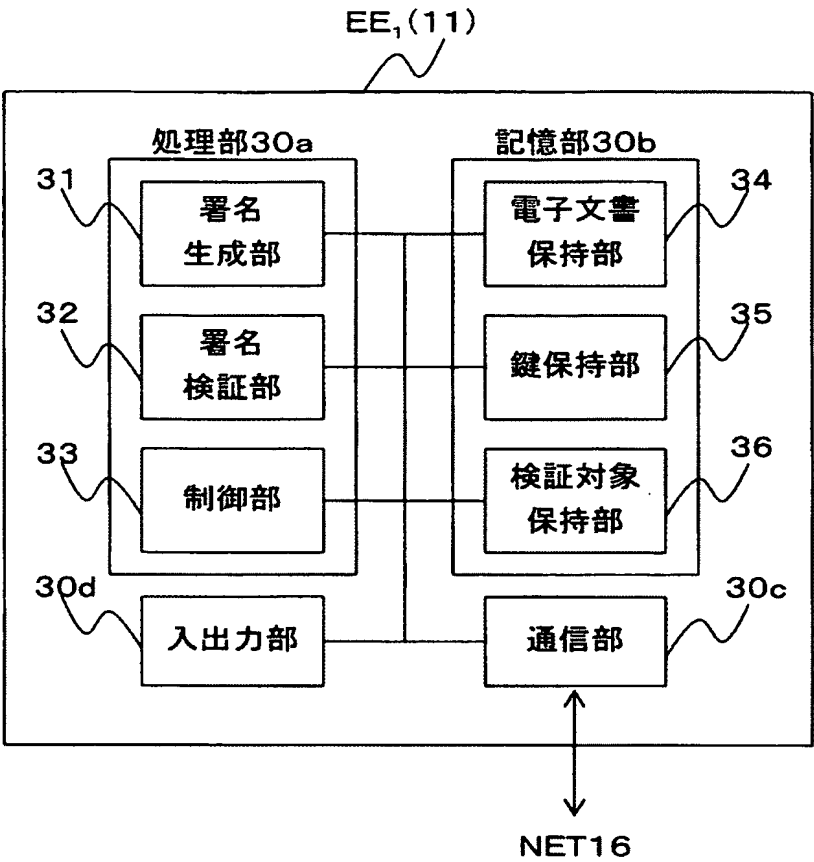
【図 2】

図 2



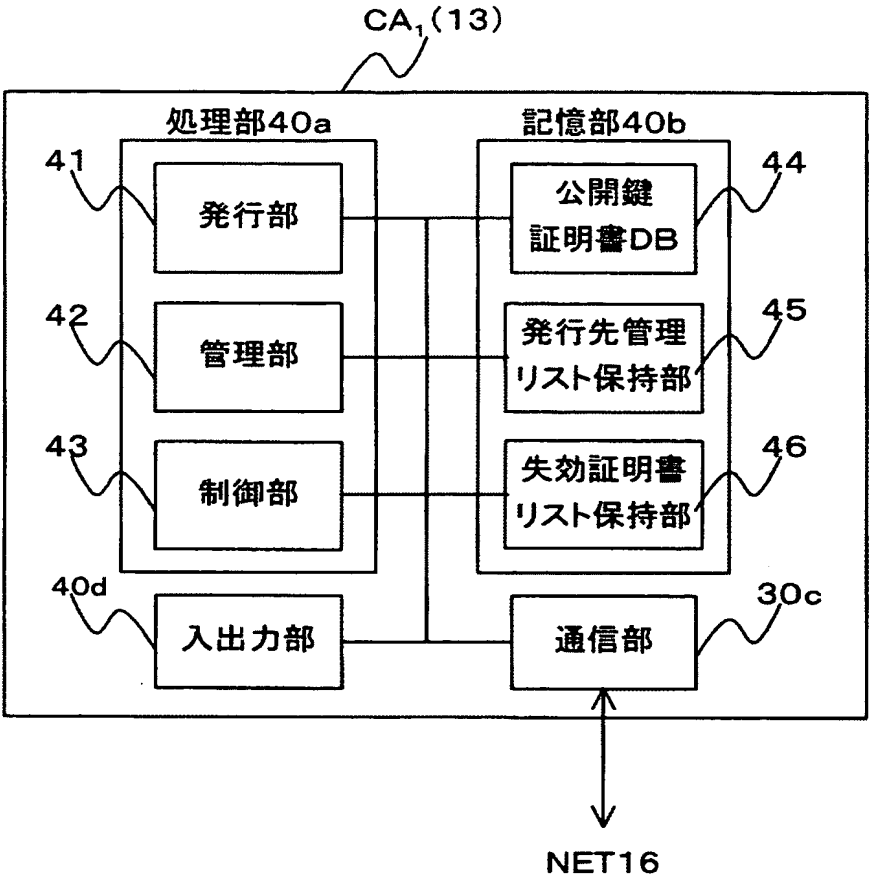
【図 3】

図 3



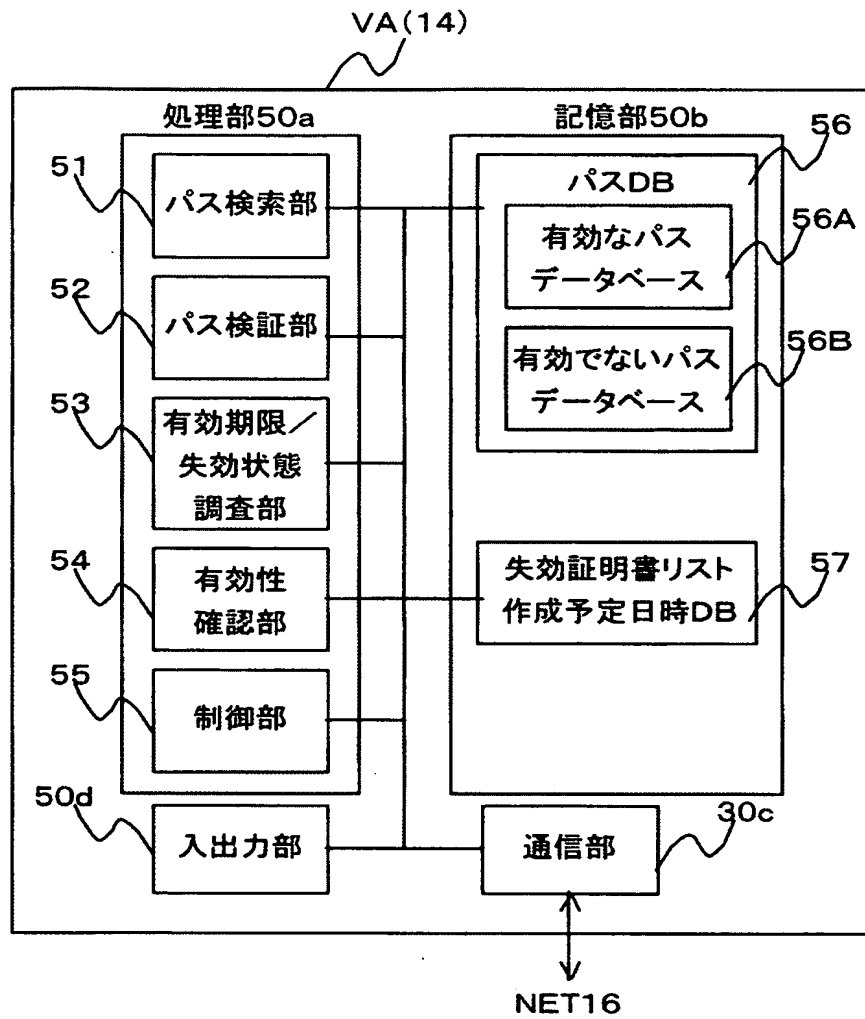
【図 4】

図 4



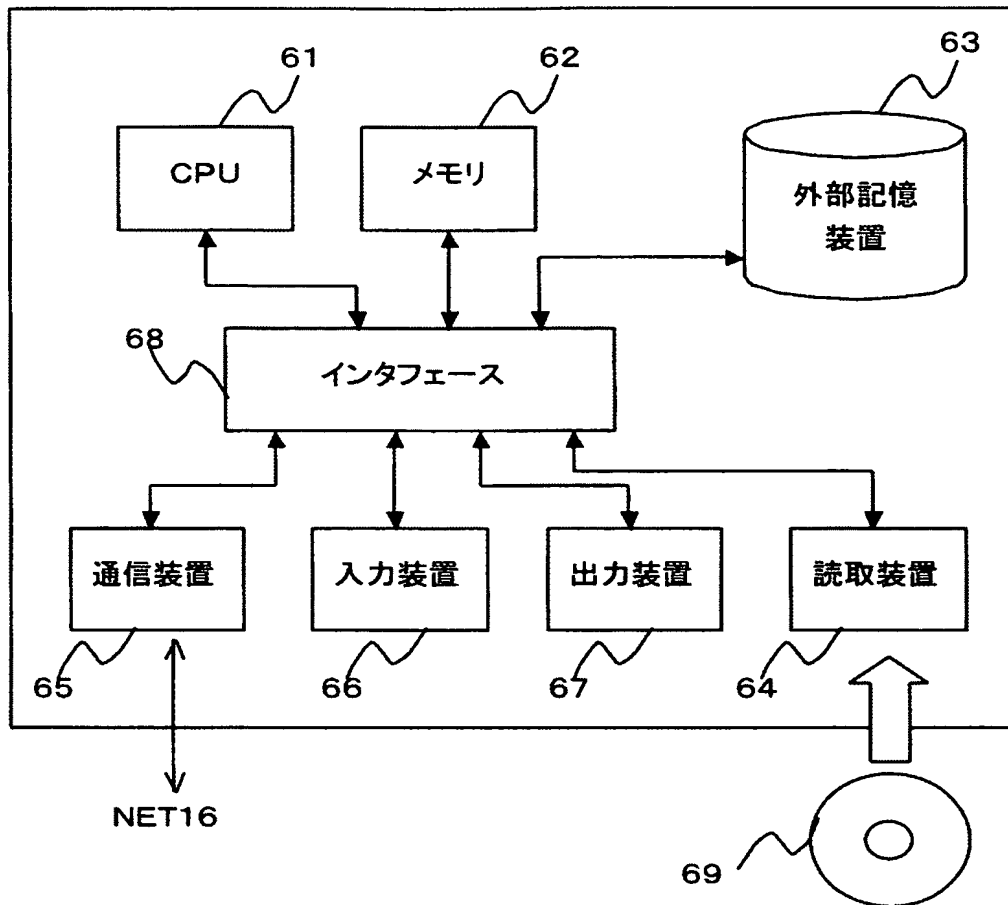
【図 5】

図 5



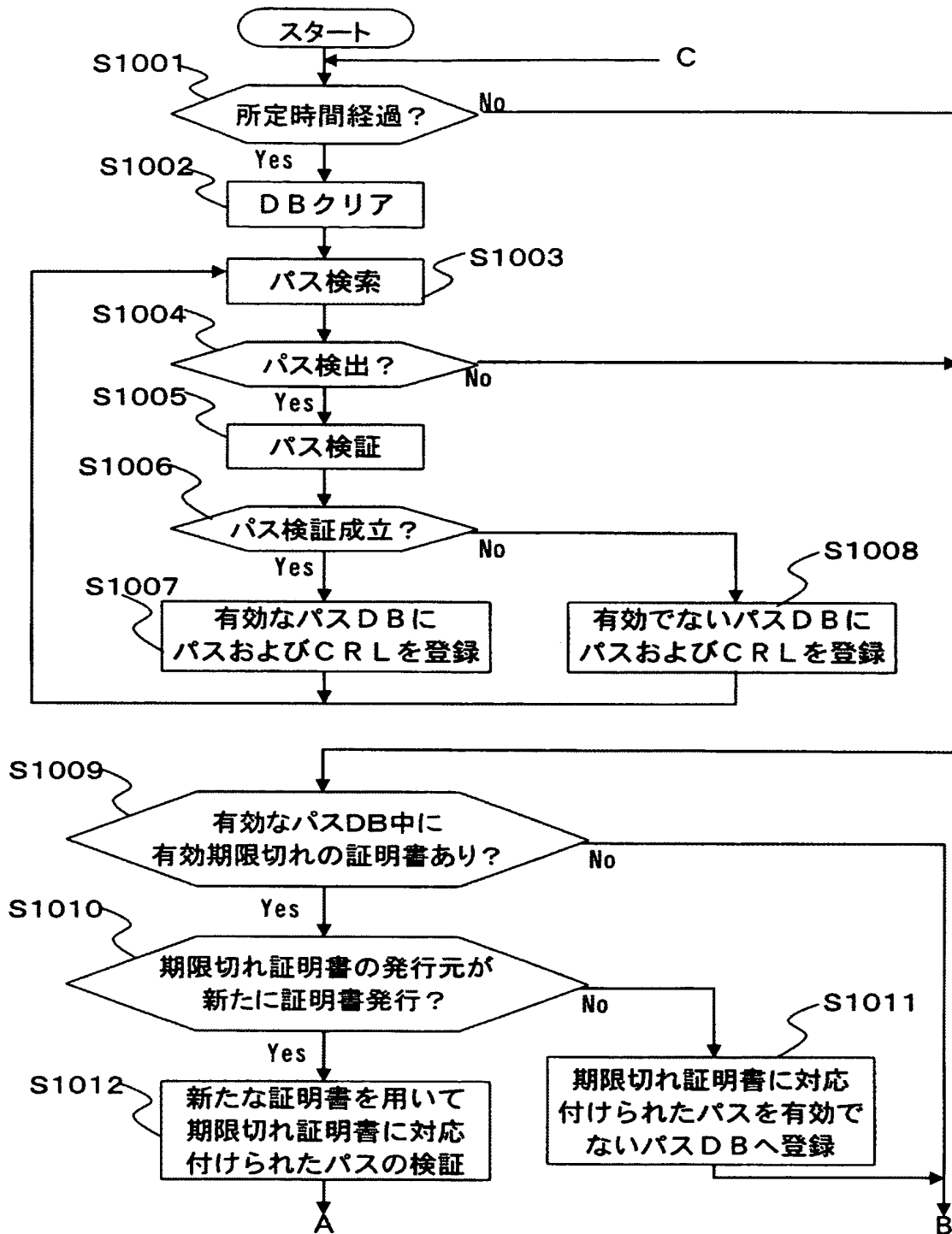
【図 6】

図 6



【図 7】

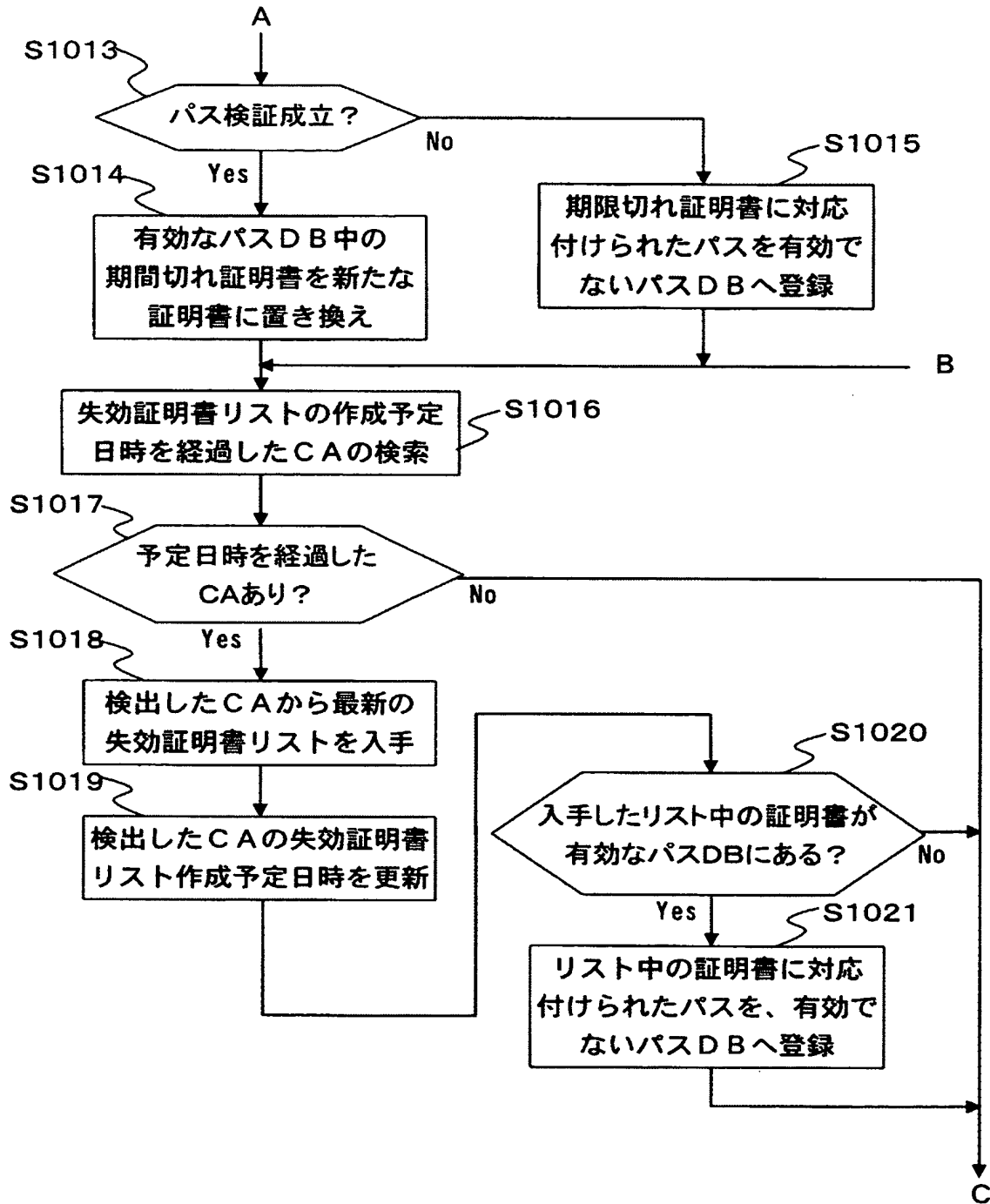
図 7 パスの検索、検証、および管理動作



【図 8】

図 8

パスの検索、検証、および管理動作



【図 9】

図 9

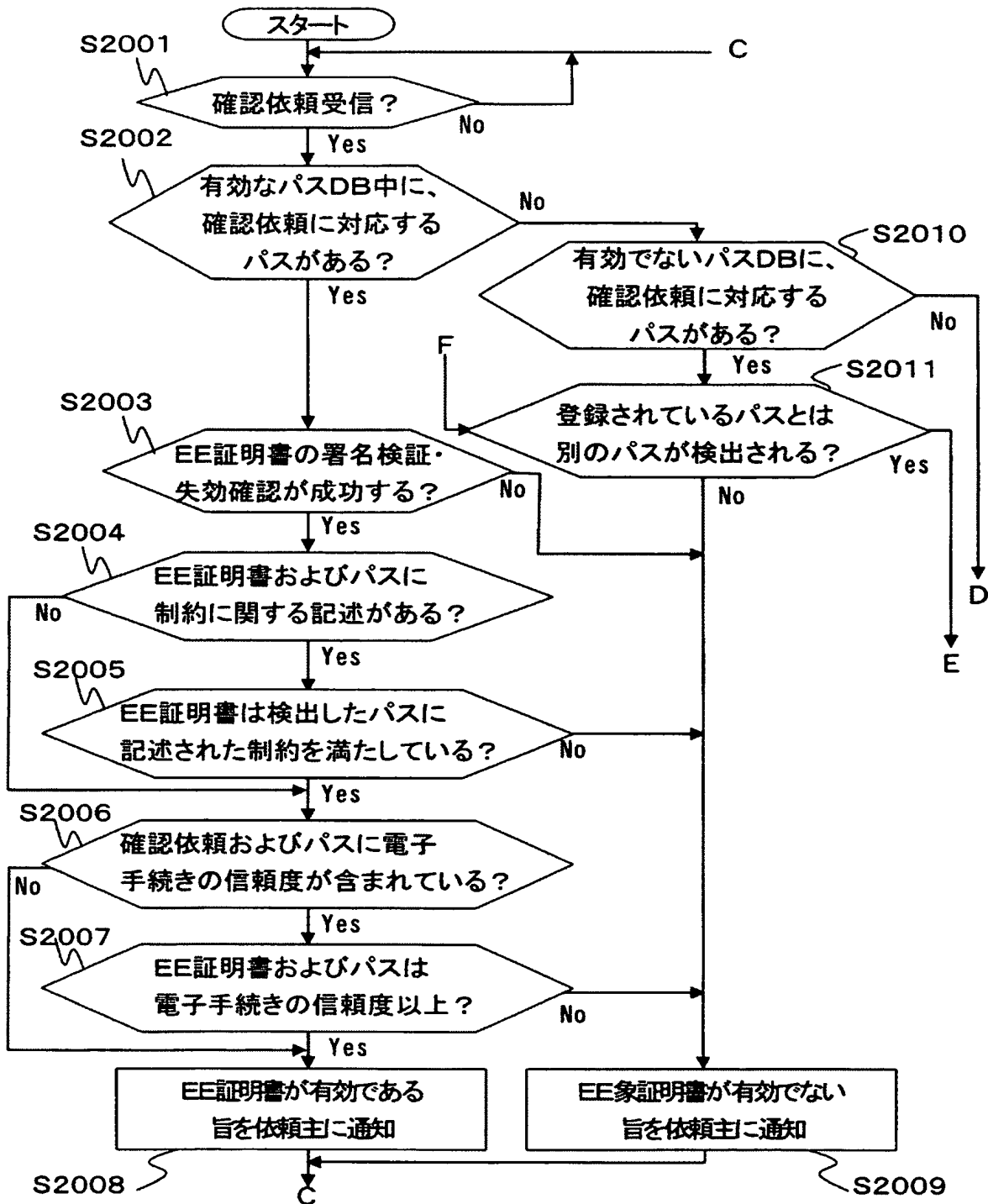
パス検索結果(図2の場合)

有効なパス			
トラスト アンカーCA	EE証明書 発行CA	パス	CRL
CA ₁₁	CA ₁₂	CA ₁₁ - CA ₁₂	有効
	CA ₂₂	CA ₁₁ - CAbridge - CA ₂₁ - CA ₂₂	有効
CA ₂₁	CA ₁₂	CA ₂₁ - CAbridge - CA ₁₁ - CA ₁₂	有効
	CA ₂₂	CA ₂₁ - CA ₂₂	有効
CAbridge	CA ₁₂	CAbridge - CA ₁₁ - CA ₁₂	有効
	CA ₂₂	CAbridge - CA ₂₁ - CA ₂₂	有効

有効でないパス			
トラスト アンカーCA	EE証明書 発行CA	パス	CRL
CA ₁₁	CA ₁₃	CA ₁₁ - CA ₁₂	無効
CA ₂₁	CA ₁₂	CA ₂₁ - CAbridge - CA ₁₁ - CA ₁₂	無効
CAbridge	CA ₁₂	CAbridge - CA ₁₁ - CA ₁₂	無効

【図 10】

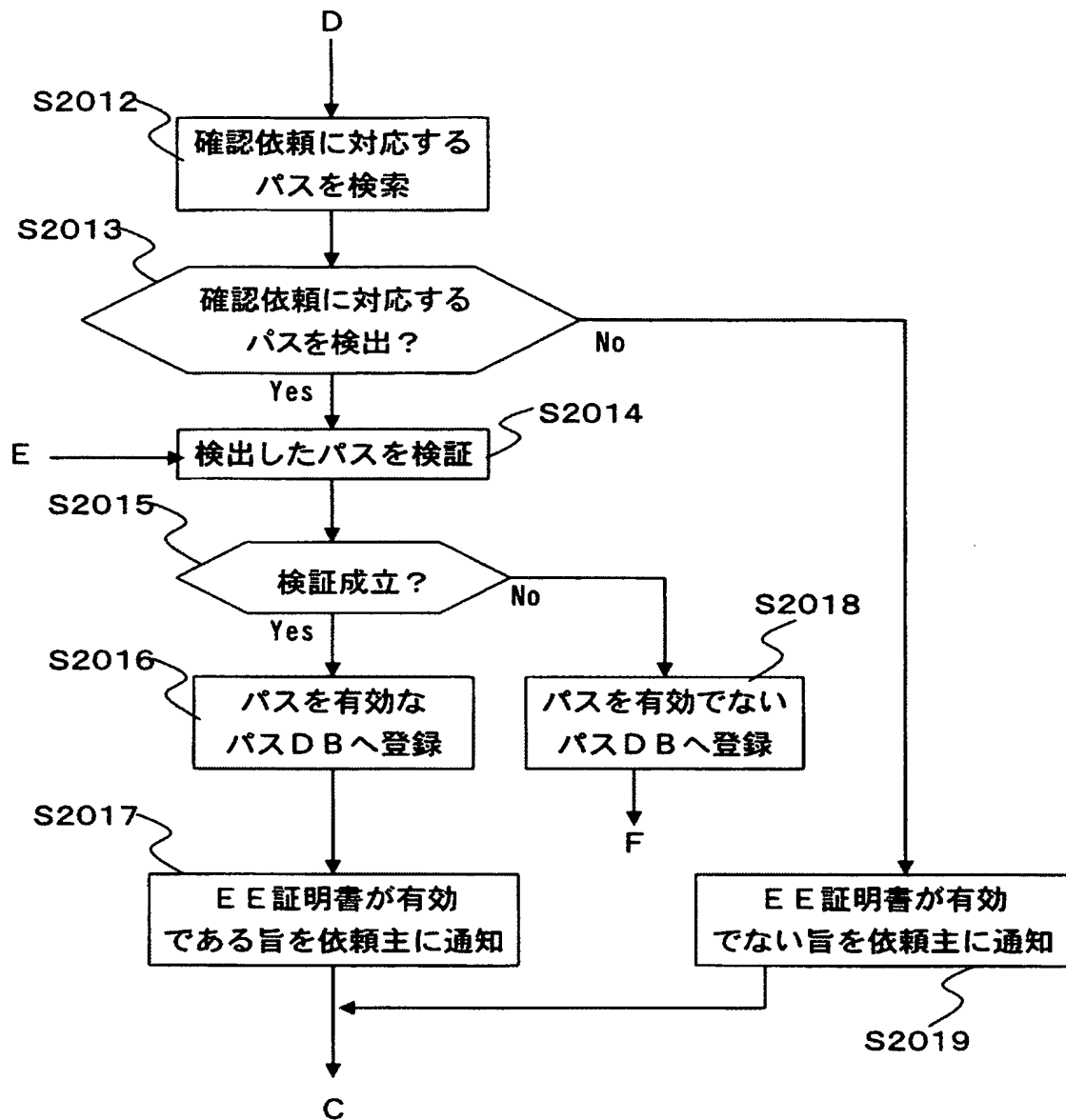
図 10 公開鍵証明書の有効性の確認動作



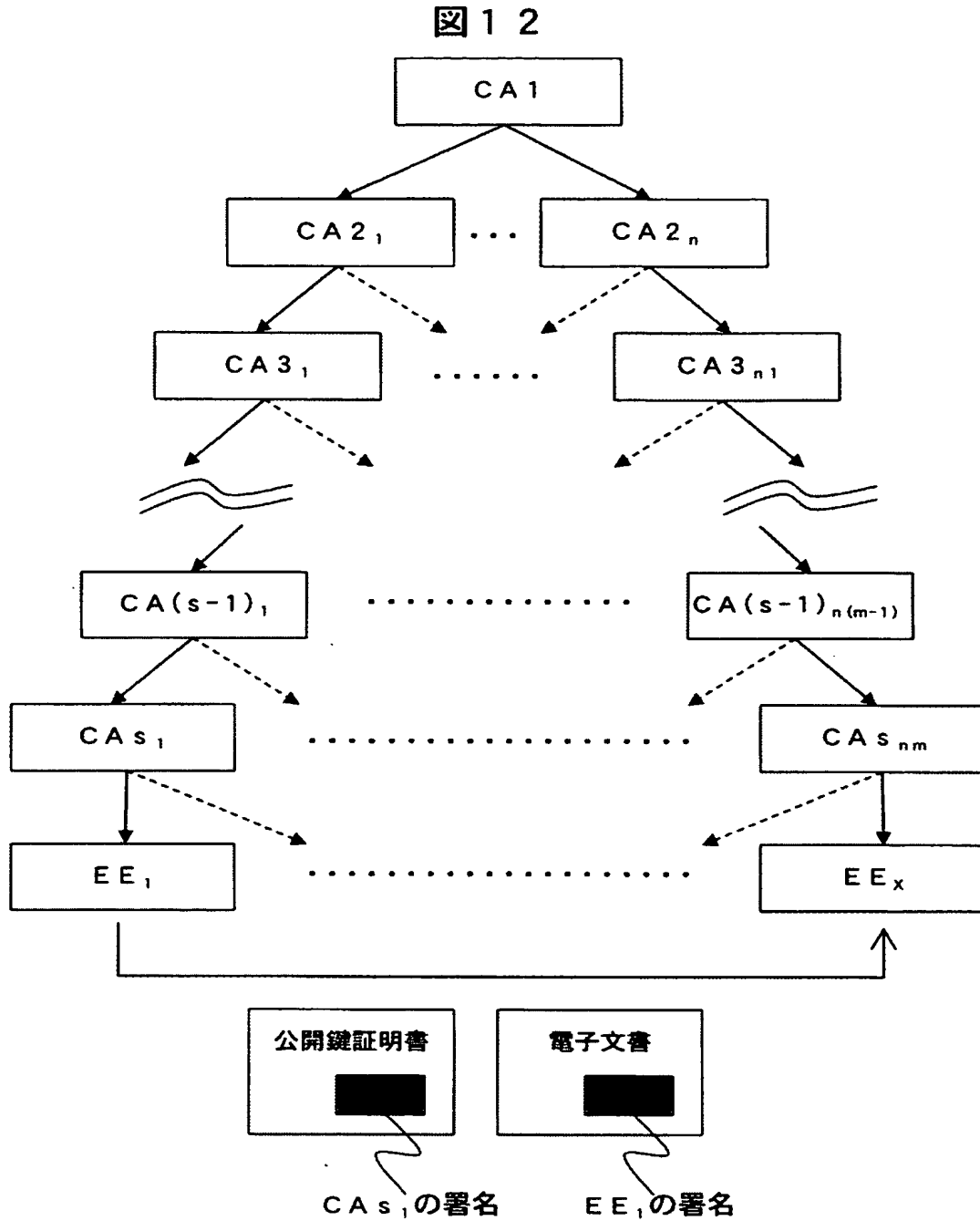
【図 11】

図 11

公開鍵証明書の有効性の確認動作



【図 12】



【書類名】 要約書**【要約】****【課題】**

パス検索時以降に新たなパスが存在する場合でも適切な結果を応答し、かつ、エンドエンティティが公開鍵証明書の有効性確認を依頼してからその結果が分かるまでにかかる時間を短縮する。

【解決手段】

証明書の有効性確認局は、予め定期的に、パスおよび失効証明書リストを検索、検証し、当該検証結果に応じて、有効なパスおよび有効でないパスに分類して、データベースへ登録する。また、エンドエンティティから証明書の有効性確認依頼があった場合、当該依頼に対応するパスが、有効なパスデータベースか、有効でないパスデータベースのどちらに登録されているかを調べ、当該公開鍵証明書の有効性を判断する。一方、当該有効性確認依頼に対応するパスがデータベースに登録されていない場合には、新たにパス検索、検証を行うことにより、当該公開鍵証明書の有効性確認を行う。

【選択図】 図 2

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 3 5 1 5 0 9
受付番号	5 0 3 0 1 6 8 9 7 0 7
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 5 年 1 0 月 1 4 日

< 認定情報・付加情報 >

【提出日】	平成15年10月10日
-------	-------------

特願 2 0 0 3 - 3 5 1 5 0 9

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日 1 9 9 0 年 8 月 3 1 日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台 4 丁目 6 番地

氏 名 株式会社日立製作所